



# Cross-Enterprise Security and Privacy Authorization (XSPA) Profile of XACML v2.0 for Healthcare Version 1.0

## Committee Specification 02

25 August 2009

### Specification URIs:

#### This Version:

<http://docs.oasis-open.org/xacml/xspa/v1.0/xacml-xspa-1.0-cs02.html>  
<http://docs.oasis-open.org/xacml/xspa/v1.0/xacml-xspa-1.0-cs02.doc> (Authoritative)  
<http://docs.oasis-open.org/xacml/xspa/v1.0/xacml-xspa-1.0-cs02.pdf>

#### Previous Version:

<http://docs.oasis-open.org/xacml/xspa/v1.0/xacml-xspa-1.0-cd04.html>  
<http://docs.oasis-open.org/xacml/xspa/v1.0/xacml-xspa-1.0-cd04.doc> (Authoritative)  
<http://docs.oasis-open.org/xacml/xspa/v1.0/xacml-xspa-1.0-cd04.pdf>

#### Latest Version:

<http://docs.oasis-open.org/xacml/xspa/v1.0/xacml-xspa-1.0.html>  
<http://docs.oasis-open.org/xacml/xspa/v1.0/xacml-xspa-1.0.doc> (Authoritative)  
<http://docs.oasis-open.org/xacml/xspa/v1.0/xacml-xspa-1.0.pdf>

#### Technical Committee:

[OASIS eXtensible Access Control Markup Language \(XACML\) TC](#)

#### Chair(s):

Hal Lockhart, Oracle Corporation  
Bill Parducci, Individual

#### Editor(s):

Duane DeCouteau, Department of Veterans Affairs  
Mike Davis, Department of Veterans Affairs  
David Staggs, Department of Veterans Affairs

#### Related work:

This specification is related to:

- [eXtensible Access Control Markup Language\(XACML\) Version 2.0](#)

#### Declared XML Namespace(s):

N/A

#### Abstract:

A profile of XACML used to support cross-enterprise security and privacy authorization.

#### Status:

This document was last revised or approved by the OASIS eXtensible Access Control Markup Language (XACML) TC on the above date. The level of approval is also listed above. Check the "Latest Version" or "Latest Approved Version" location noted above for possible later revisions of this document.

Technical Committee members should send comments on this specification to the Technical Committee's email list. Others should send comments to the Technical Committee by using the "Send A Comment" button on the Technical Committee's web page at <http://www.oasis-open.org/committees/xacml/> .

For information on whether any patents have been disclosed that may be essential to implementing this specification, and any offers of patent licensing terms, please refer to the Intellectual Property Rights section of the Technical Committee web page (<http://www.oasis-open.org/committees/xacml/ipr.php> .

The non-normative errata page for this specification is located at <http://www.oasis-open.org/committees/xacml/> .

---

## Notices

Copyright © OASIS® 2008-2009. All Rights Reserved.

All capitalized terms in the following text have the meanings assigned to them in the OASIS Intellectual Property Rights Policy (the "OASIS IPR Policy"). The full Policy may be found at the OASIS website.

This document and translations of it may be copied and furnished to others, and derivative works that comment on or otherwise explain it or assist in its implementation may be prepared, copied, published, and distributed, in whole or in part, without restriction of any kind, provided that the above copyright notice and this section are included on all such copies and derivative works. However, this document itself may not be modified in any way, including by removing the copyright notice or references to OASIS, except as needed for the purpose of developing any document or deliverable produced by an OASIS Technical Committee (in which case the rules applicable to copyrights, as set forth in the OASIS IPR Policy, must be followed) or as required to translate it into languages other than English.

The limited permissions granted above are perpetual and will not be revoked by OASIS or its successors or assigns.

This document and the information contained herein is provided on an "AS IS" basis and OASIS DISCLAIMS ALL WARRANTIES, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO ANY WARRANTY THAT THE USE OF THE INFORMATION HEREIN WILL NOT INFRINGE ANY OWNERSHIP RIGHTS OR ANY IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE.

OASIS requests that any OASIS Party or any other party that believes it has patent claims that would necessarily be infringed by implementations of this OASIS Committee Specification or OASIS Standard, to notify OASIS TC Administrator and provide an indication of its willingness to grant patent licenses to such patent claims in a manner consistent with the IPR Mode of the OASIS Technical Committee that produced this specification.

OASIS invites any party to contact the OASIS TC Administrator if it is aware of a claim of ownership of any patent claims that would necessarily be infringed by implementations of this specification by a patent holder that is not willing to provide a license to such patent claims in a manner consistent with the IPR Mode of the OASIS Technical Committee that produced this specification. OASIS may include such claims on its website, but disclaims any obligation to do so.

OASIS takes no position regarding the validity or scope of any intellectual property or other rights that might be claimed to pertain to the implementation or use of the technology described in this document or the extent to which any license under such rights might or might not be available; neither does it represent that it has made any effort to identify any such rights. Information on OASIS' procedures with respect to rights in any document or deliverable produced by an OASIS Technical Committee can be found on the OASIS website. Copies of claims of rights made available for publication and any assurances of licenses to be made available, or the result of an attempt made to obtain a general license or permission for the use of such proprietary rights by implementers or users of this OASIS Committee Specification or OASIS Standard, can be obtained from the OASIS TC Administrator. OASIS makes no representation that any information or list of intellectual property rights will at any time be complete, or that any claims in such list are, in fact, Essential Claims.

The names "OASIS", "XSPA", and "XACML" are trademarks of OASIS, the owner and developer of this specification, and should be used only to refer to the organization and its official outputs. OASIS welcomes reference to, and implementation and use of, specifications, while reserving the right to enforce its marks against misleading uses. Please see <http://www.oasis-open.org/who/trademark.php> for above guidance.

---

# Table of Contents

1	Introduction.....	5
1.1	Terminology .....	5
1.2	Normative References .....	6
1.3	Non-Normative References .....	6
2	2 XSPA profile of XACML.....	7
2.1	Interactions between Parties .....	7
2.1.1	Service Interface .....	7
2.1.2	Access Control Service (Service Consumer) .....	7
2.1.3	Attribute Service .....	7
2.1.4	Policy Authority.....	7
2.1.5	Access Control Service (Service Provider) .....	8
2.2	Transmission Integrity.....	8
2.3	Transmission Confidentiality.....	8
2.4	Error States.....	8
2.5	Security Considerations.....	8
2.6	Confirmation Identifiers.....	8
2.7	Metadata Definitions .....	8
2.8	Naming Syntax, Restrictions and Acceptable Values .....	8
2.9	Namespace Requirements .....	9
2.10	Attribute Rules of Equality .....	9
2.11	Attribute Naming Syntax, Restrictions and Acceptable Values.....	9
2.12	Standard Rules (Normative) .....	14
2.13	Standard Rules (Non-normative).....	14
2.14	Obligations (Normative) .....	14
2.15	Obligations (Non-normative).....	14
2.16	Examples of Use.....	14
3	Conformance .....	17
3.1	Introduction .....	17
3.2	Conformance Tables .....	17
3.2.1	Attributes .....	17
A.	Acknowledgements .....	20
B.	Revision History.....	21

---

# Table of Figures

Figure 1:	Interaction between Parties .....	7
-----------	-----------------------------------	---

---

# 1 Introduction

Enterprises, including the healthcare enterprise, need a mechanism to exchange security and privacy policies, evaluate consent directives and determine authorizations in an interoperable manner. This document provides a cross-enterprise security and privacy profile that describes how to use eXtensible Access Control Markup Language (XACML) to provide these functions in an interoperable manner.

The Cross-Enterprise Security and Privacy Authorization (XSPA) profile of XACML describes several mechanisms to authenticate, administer, and enforce authorization policies controlling access to protected information residing within or across enterprise boundaries. The policies being administered and enforced relate to security, privacy, and consent directives. This profile MAY be used in coordination with additional standards including Web Services Trust Language (WS-Trust) and Security Assertion Markup Language (SAML).

This profile specifies the use of XACML 2.0 to promote interoperability within the healthcare community by providing common semantics and vocabularies for interoperable policy request/response, policy lifecycle, and policy enforcement.

## 1.1 Terminology

The key words “MUST”, “MUST NOT”, “REQUIRED”, “SHALL”, “SHALL NOT”, “SHOULD”, “SHOULD NOT”, “RECOMMENDED”, “MAY”, and “OPTIONAL” in this document are to be interpreted as described in [RFC2119].

The following definitions establish additional terminology and usage in this profile:

**Access Control Service (ACS)** – The enterprise security service that supports and implements user-side and service-side access control capabilities. The service would be utilized by the Service and/or Service User.

**Entity** – A principal and/or subject, which represents an application, a machine, or any other type of entity that may act as a requester in a transaction.

**Object** – An entity that contains or receives information. Objects can represent information containers (e.g., files or directories in an operating system, and/or columns, rows, tables, and views within a database management system) or represent exhaustible system resources, such as printers, disk space, and central processing unit (CPU) cycles.

**Operation** - An executable image of a program, which upon invocation executes some function for the user. Within a file system, operations might include read, write, and execute. Within a database management system, operations might include insert, delete, append, and update. An operation is also known as an action or privilege.

**Permission** - An approval to perform an operation on one or more protected objects.

**Policy Administration Point (PAP)** – Manages and makes available policies that may be stored in and retrieved from the Policy Repository.

**Policy Decision Point (PDP)** – Accepts information from an Authorization Decision Request and returns an access control decision based on evaluation of XACML policy. PDPs MAY be hierarchical.

**Policy Enforcement Point (PEP)** – Performs access control by making decision requests and enforcing authorization decisions. It facilitates passing XACML authorization request attributes and enforcing XACML response decisions and obligations. This module MAY be used for obtaining attributes required for authorization from a Policy Information Point (PIP) by an application. Typical attributes collected at this level include ANSI RBAC (American National Standards Institute Role Based Access Control) attributes, Health Level Seven (HL7) provider permissions, HL7 resource permission, and HL7 patient privacy constraints.

**Policy Information Point (PIP)** – Repository of attribute data that is made available to support authorization decisions.

47 **Structural Role** - A job function within the context of an organization whose permissions are defined by  
48 operations on workflow objects consistent with the definition of structural role found in ASTM (American  
49 Society for Testing and Materials) [E2595-2007]  
50 **Service Provider (SP)** - The service provider represents the system providing a protected resource and  
51 relies on the provided security service.  
52 **Service User** – The service user represents any individual entity [such as on an Electronic Health Record  
53 (EHR)/personal health record (PHR) system] that needs to make a service request of a Service Provider.

## 54 1.2 Normative References

55 **[RFC2119]** S. Bradner, *Key words for use in RFCs to Indicate Requirement Levels*,  
56 <http://www.ietf.org/rfc/rfc2119.txt>, IETF RFC 2119, March 1997.  
57 **[XACML CORE]** OASIS Standard, "XACML 2.0 Core: eXtensible Access Control Markup  
58 Language (XACML) Version 2.0", March 2005  
59 [http://docs.oasis-open.org/xacml/2.0/access\\_control-xacml-2.0-core-spec-os.pdf](http://docs.oasis-open.org/xacml/2.0/access_control-xacml-2.0-core-spec-os.pdf)  
60 **[SAML-XACML20]** OASIS Working Draft, "SAML 2.0 profile of XACML 2.0 Errata", November 2005,  
61 [http://www.oasis-open.org/committees/download.php/15447/xacml-2.0-saml-](http://www.oasis-open.org/committees/download.php/15447/xacml-2.0-saml-errata-wd.zip)  
62 [errata-wd.zip](http://www.oasis-open.org/committees/download.php/15447/xacml-2.0-saml-errata-wd.zip)  
63 **[SX20-ASSN-SCH]** OASIS Standard, schema (assertion), [http://www.oasis-](http://www.oasis-open.org/committees/download.php/11474/access_control-xacml-2.0-saml-assertion-schema-os.xsd)  
64 [open.org/committees/download.php/11474/access\\_control-xacml-2.0-saml-](http://www.oasis-open.org/committees/download.php/11474/access_control-xacml-2.0-saml-assertion-schema-os.xsd)  
65 [assertion-schema-os.xsd](http://www.oasis-open.org/committees/download.php/11474/access_control-xacml-2.0-saml-assertion-schema-os.xsd)  
66 **[SX20-PROT-SCH]** OASIS Standard, schema (protocol), [http://www.oasis-](http://www.oasis-open.org/committees/download.php/11475/access_control-xacml-2.0-saml-protocol-schema-os.xsd)  
67 [open.org/committees/download.php/11475/access\\_control-xacml-2.0-saml-](http://www.oasis-open.org/committees/download.php/11475/access_control-xacml-2.0-saml-protocol-schema-os.xsd)  
68 [protocol-schema-os.xsd](http://www.oasis-open.org/committees/download.php/11475/access_control-xacml-2.0-saml-protocol-schema-os.xsd)  
69 **[HL7-PERM]** HL7 Security Technical Committee, HL7 Version 3 Standard: Role-based Access  
70 Control Healthcare Permission Catalog, (Available through  
71 <http://www.hl7.org/library/standards.cfm>), Release 1, Designation: ANSI/HL7 V3  
72 RBAC, R1-2008.  
73 **[HL7-CONSENT]** HL7 Consent Related Vocabulary Confidentiality Codes Recommendation,  
74 <http://lists.oasis-open.org/archives/xacml-demo-tech/200712/doc00003.doc>, from  
75 project submission: [http://lists.oasis-open.org/archives/xacml-demo-](http://lists.oasis-open.org/archives/xacml-demo-tech/200712/msg00015.html)  
76 [tech/200712/msg00015.html](http://lists.oasis-open.org/archives/xacml-demo-tech/200712/msg00015.html)  
77 **[ASTM E1986-98 (2005)]** Standard Guide for Information Access Privileges to Health Information.  
78 **[ASTM E2595 (2007)]** Standard Guide for Privilege Management Infrastructure  
79 **[XSPA-SAML]** OASIS Committee Draft 04, "Cross-Enterprise Security and Privacy Authorization  
80 (XSPA) Profile of Security Assertion Markup Language (SAML) v2.0 for  
81 Healthcare Version 1.0" July 2009 [http://docs.oasis-open.org/xspa/1.0/saml-](http://docs.oasis-open.org/xspa/1.0/saml-xspa-1.0-cd04.doc)  
82 [xspa-1.0-cd04.doc](http://docs.oasis-open.org/xspa/1.0/saml-xspa-1.0-cd04.doc)

## 83 1.3 Non-Normative References

84 **[SAML-XACML20V2]** OASIS Working Draft, "SAML 2.0 profile of XACML Version 2", July 2007  
85 (current working draft covers all versions of XACML).  
86 [http://www.oasis-open.org/committees/download.php/24681/xacml-profile-](http://www.oasis-open.org/committees/download.php/24681/xacml-profile-saml2.0-v2-spec-wd-5-en.pdf)  
87 [saml2.0-v2-spec-wd-5-en.pdf](http://www.oasis-open.org/committees/download.php/24681/xacml-profile-saml2.0-v2-spec-wd-5-en.pdf)  
88 **[XACML-RBAC]** OASIS Standard, "Core and hierarchical role based access control (RBAC)  
89 profile of XACML v2.0", February 2005  
90 [http://docs.oasis-open.org/xacml/2.0/access\\_control-xacml-2.0-rbac-profile1-](http://docs.oasis-open.org/xacml/2.0/access_control-xacml-2.0-rbac-profile1-spec-os.pdf)  
91 [spec-os.pdf](http://docs.oasis-open.org/xacml/2.0/access_control-xacml-2.0-rbac-profile1-spec-os.pdf)  
92 **[HITSP]** Healthcare Information Technology Standards Panel (HITSP) at [www.hitsp.org](http://www.hitsp.org)  
93 **[XSPA-XACML-EXAMPLES]** Cross-Enterprise Security and Privacy Authorization (XSPA)  
94 Profile of XACML v2.0 for Healthcare, Implementation Examples.  
95 [http://www.oasis-open.org/committees/document.php?document\\_id=30430](http://www.oasis-open.org/committees/document.php?document_id=30430)

## 2 XSPA profile of XACML

### 2.1 Interactions between Parties

Figure 1 displays an overview of interactions between parties in the exchange of healthcare information. Elements described in the figure are explained in the subsections below.

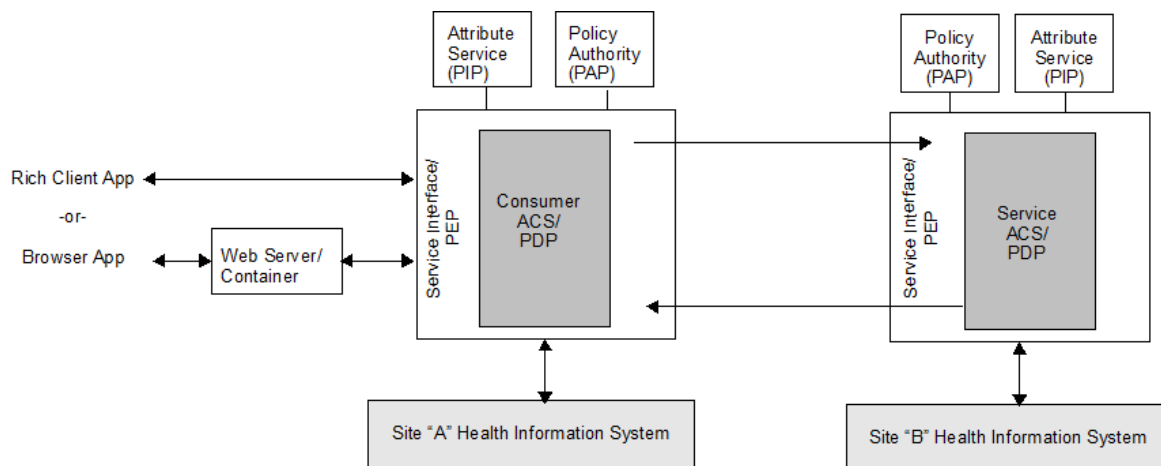


Figure 1: Interaction between Parties

#### 2.1.1 Service Interface

XACML functions of the Policy Enforcement Point (PEP) are carried out by the Service Interface.

The PEP interacts with the Policy Information Point (PIP) of the Attribute Service and the Policy Decision Point (PDP) functionality of the Access Control Service (ACS), in enforcing authorization decisions.

#### 2.1.2 Access Control Service (Service Consumer)

The XSPA profile of XACML supports sending all Service User requests through an ACS. XACML functions of the PDP are carried out by the ACS. The Service Consumer ACS MAY serve as an enterprise gateway.

Attributes necessary to make a local access control decision are determined and HL7 Permission [HL7-PERM] are granted to the Service User based on their role, purpose of use (POU), the service endpoint of the external resource, and any site specific operational attributes.

#### 2.1.3 Attribute Service

XACML functions of the Policy Information Point (PIP) are carried out by the Attribute Service.

The Attribute Service has access to attribute information (e.g., location, purpose of use), object preferences, consent directives and other privacy conditions (object masking, object filtering, user, role, purpose, etc.) that constrain enforcement.

#### 2.1.4 Policy Authority

XACML functions of the Policy Administration Point (PAP) are carried out by the Policy Authority.

The Policy Authority has access to security policies that include rules regarding authorizations required to access a protected resource and additional security conditions (location, time of day, cardinality, separation of duty purpose, etc.) that constrain enforcement.

### 124 **2.1.5 Access Control Service (Service Provider)**

125 The Service ACS is responsible for the parsing of assertions, evaluating the assertions against the  
126 security and privacy policy, and making and enforcing a decision on behalf of the Service Provider. The  
127 Service ACS MAY serve as an enterprise gateway.

### 128 **2.2 Transmission Integrity**

129 The XSPA profile of XACML recommends the use of reliable transmission protocols. Where transmission  
130 integrity is required, this profile makes no specific recommendations regarding mechanism or assurance  
131 level.

### 132 **2.3 Transmission Confidentiality**

133 The XSPA profile of XACML recommends the use of secure transmission protocols. Where transmission  
134 confidentiality is required, this profile makes no specific recommendations regarding mechanisms.

### 135 **2.4 Error States**

136 This profile adheres to error states described in **[XACML-CORE]**.

### 137 **2.5 Security Considerations**

138 The following security considerations are established for the XSPA profile of XACML:

- 139 • Entities MUST be members of defined information domains under the authorization control of a  
140 defined set of policies,
- 141 • Entities MUST have been identified and provisioned (credentials issued, privileges granted, etc.) in  
142 accordance with policy,
- 143 • Privacy policies MUST have been identified and provisioned (consents, user preferences, etc.) in  
144 accordance with policy,
- 145 • Pre-existing security and privacy policies MUST have been provisioned to Access Control Services,
- 146 • The capabilities and location of requested information/document repository services MUST be known,
- 147 • Secure channels MUST be established as required by policy,
- 148 • Audit services MUST be operational and initialized, and
- 149 • Entities MUST have pre-asserted membership in an information domain by successful and unique  
150 authentication.

### 151 **2.6 Confirmation Identifiers**

152 The manner used by the relying party to confirm that the requester message came from a system entity  
153 that is associated with the subject of the assertion will depend upon the context and sensitivity of the  
154 data. For confirmations requiring a specific level of assurance, this profile specifies the use of National  
155 Institute of Standards and Technology (NIST) Special Publication 800-63 Electronic Authentication  
156 Guideline. In addition, this profile specifies the Liberty Identity Access Framework (LIAF) criteria for  
157 evaluating and approving credential service providers.

### 158 **2.7 Metadata Definitions**

159 A XACML extension is used to enable the SAML protocol layer. This is described in the **[SAML-XACML-**  
160 **20]** specification and in the **[SX20-PROT-SCH]** schema.

### 161 **2.8 Naming Syntax, Restrictions and Acceptable Values**

162 This profile will support the namespace requirements described in **[XACML-CORE]**.

163 **2.9 Namespace Requirements**

164 This profile will support the namespace requirements described in [XACML-CORE].

165 **2.10 Attribute Rules of Equality**

166 This profile will support the attribute evaluation requirements described in [XACML-CORE].

167 **2.11 Attribute Naming Syntax, Restrictions and Acceptable Values**

168 *Table 1: Standard Attributes (Normative)*

Attribute ID*	Identifier	Type	Valid Values
subject:subject-id	urn:oasis:names:tc:xacml:1.0:subject:subject-id	String	Is the name of the user as required by Health Insurance Portability and Accountability Act (HIPAA) Privacy Disclosure Accounting. The name will be typed as a string and in plain text.
subject:organization	urn:oasis:names:tc:xspa:1.0:subject:organization	String	Organization the requesting user belongs to as required by Health Insurance Portability and Accountability Act (HIPAA) Privacy Disclosure Accounting. The name will be typed as a string and in plain text.
subject:organization-id	urn:oasis:names:tc:xspa:1.0:subject:organization-id	anyURI	Unique identifier of the consuming organization and/or facility
subject:hl7:permission	urn:oasis:names:tc:xspa:1.0:subject:hl7:permission	String	Refer to [HL7-PERM] and its OID representation.
subject:role	urn:oasis:names:tc:xacml:2.0:subject:role	String	Structural Role refer to [ASTM E1986-98 (2005)] and its OID representation.
subject:purposeofuse	urn:oasis:names:tc:xspa:1.0:subject:purposeofuse	String	TREATMENT, PAYMENT, OPERATIONS, EMERGENCY, MARKETING, RESEARCH, REQUEST, PUBLICHEALTH
resource:resource-id	urn:oasis:names:tc:xacml:1.0:resource:resource-id	String	Unique identifier of the resource defined by and controlled by the servicing organization. In healthcare this is the patient unique identifier.

Attribute ID*	Identifier	Type	Valid Values
resource:hl7:type	urn:oasis:names:tc:xspa:1.0:resource:hl7:type	String	For minimum interoperability set of objects and supporting actions refer to [HL7-PERM] and their OID representations.
resource:org:permission	urn:oasis:names:tc:xspa:1.0:resource:org:hl7:permissions	String	Refer to [HL7-PERM] and its OID representation. This attribute holds permissions required by the servicing organization to grant access to a specific resource.
resource:org:role	urn:oasis:names:tc:xspa:1.0:resource:org:role	String	Structural Role refer to [ASTM E1986-98 (2005)] and its OID representation. This attribute holds roles required by the servicing organization to grant access to a specific resource.
resource:patient:confidentiality-code	urn:oasis:names:tc:xspa:1.0:resource:patient:hl7:confidentiality-code	String	Refer to [HL7-CONSENT] The default value for this attribute is N (normal operations.)
resource:hl7:dissenting-subject-id	urn:oasis:names:tc:xspa:1.0:resource:patient:dissenting-subject-id	String	US domain specific is National Provider issued by HHS/CMS and mandated by HIPAA.
resource:hl7:dissenting-role	urn:oasis:names:tc:xspa:1.0:resource:patient:dissenting-role	String	Structural Role refer to [ASTM E1986-98 (2005)] and its OID representation.
environment:locality	urn:oasis:names:tc:xspa:1.0:environment:locality	String	Unique identifier of the servicing organization.

169 \*Note: Attribute-ID is provided for mapping to pseudo-code in the [XSPA-XACML-EXAMPLES] document.

170 \*Note: The OID for the HL7 Permission Catalog [HL7-PERM] is 2.16.840.1.113883.13.27. The OID for  
171 structural roles referenced in [ASTM E1986-98 (2005)] is 1.2.840.10065.1986.7

172

173 The confidentiality-code may be used to identify sensitive information, such as records relating to drug  
174 abuse, alcoholism, or alcohol abuse, infection with the human immunodeficiency virus (HIV) or sickle cell  
175 anemia.

176 The mechanism used to identify the patient in a standardized way, e.g. resource:resource-id, is outside  
177 the scope of the profile.

178 The dissenting-subject-id identifies those denied access to a protected resource based on a patient's  
179 consent directive. The format of dissenting-subject-id MUST be consistent with the format of the subject-  
180 id.

181 HL7 RBAC Permission Catalog [HL7-PERM] represents a conformant minimum interoperability set for  
182 object/action pairings.

183

184

Table 2: Standard Attributes (Non-Normative)

Attribute ID*	Identifier	Type	Valid Values
subject:npi	urn:oasis:names:tc:xspa:1.0:subject:npi	String	National Provider ID provided by U.S. Government for all active providers.
subject:functional-role	urn:oasis:names:tc:xspa:1.0:subject:functional-role	String	Functional roles provide a placeholder to group permissions required for fine grain access control. There MUST be mutual agreement of there use and definition between participating organizations.
resource:org:allowed-organizations	urn:oasis:names:tc:xspa:1.0:resource:org:allowed-organizations	String	Holds identification of allowed trading partners.
resource:org:hoursofoperations:start	urn:oasis:names:tc:xspa:1.0:resource:org:hoursofoperations:start	Time	Time plus locale
resource:org:hoursofoperations:end	urn:oasis:names:tc:xspa:1.0:resource:org:hoursofoperations:end	Time	Time plus locale
resource:patient:opt-in	urn:gov:hhs:fa:nhinc:patient-opt-in	String	Yes or No. US realm specific and required for v2.1 of NHIN connect.
resource:patient:allowed-organizations	urn:oasis:names:tc:xspa:1.0:resource:patient:allowed-organizations	String	Holds identification of organizations allowed to access patients medical record as defined by patient's consent directive.
obligation:patient:mask:advancedirectives:dissenting-role	urn:oasis:names:tc:xspa:1.0:resource:patient:masked:advancedirectives:dissenting-role	String	Structural Role refer to [ASTM E1986-98 (2005)] and its OID representation.
obligation:patient:mask>alerts:dissenting-role	urn:oasis:names:tc:xspa:1.0:resource:patient:masked>alerts:dissenting-role	String	Structural Role refer to [ASTM E1986-98 (2005)] and its OID representation.
obligation:patient:mask:encounters:dissenting-role	urn:oasis:names:tc:xspa:1.0:resource:patient:masked:encounters:dissenting-role	String	Structural Role refer to [ASTM E1986-98 (2005)] and its OID representation.
obligation:patient:mask:familyhistory:dissenting-role	urn:oasis:names:tc:xspa:1.0:resource:patient:masked:familyhistory:dissenting-role	String	Structural Role refer to [ASTM E1986-98 (2005)] and its OID representation.
obligation:patient:mask:functionalstatus:dissenting-role	urn:oasis:names:tc:xspa:1.0:resource:patient:masked:functionalstatus:dissenting-role	String	Structural Role refer to [ASTM E1986-98 (2005)] and its OID representation.
obligation:patient:mask:immunizations:dissenting-role	urn:oasis:names:tc:xspa:1.0:resource:patient:masked:immunizations:dissenting-role	String	Structural Role refer to [ASTM E1986-98 (2005)] and its OID representation.

Attribute ID*	Identifier	Type	Valid Values
obligation:patient:mask:medicalequipment:dissenting-role	urn:oasis:names:tc:xspa:1.0:resource:patient:masked:medicalequipment:dissenting-role	String	Structural Role refer to [ASTM E1986-98 (2005)] and its OID representation.
obligation:patient:mask:medications:dissenting-role	urn:oasis:names:tc:xspa:1.0:resource:patient:masked:medications:dissenting-role	String	Structural Role refer to [ASTM E1986-98 (2005)] and its OID representation.
obligation:patient:mask:payers:dissenting-role	urn:oasis:names:tc:xspa:1.0:resource:patient:masked:payers:dissenting-role	String	Structural Role refer to [ASTM E1986-98 (2005)] and its OID representation.
obligation:patient:mask:planofcare:dissenting-role	urn:oasis:names:tc:xspa:1.0:resource:patient:masked:planofcare:dissenting-role	String	Structural Role refer to [ASTM E1986-98 (2005)] and its OID representation.
obligation:patient:mask:problems:dissenting-role	urn:oasis:names:tc:xspa:1.0:resource:patient:masked:problems:dissenting-role	String	Structural Role refer to [ASTM E1986-98 (2005)] and its OID representation.
obligation:patient:mask:procedures:dissenting-role	urn:oasis:names:tc:xspa:1.0:resource:patient:masked:procedures:dissenting-role	String	Structural Role refer to [ASTM E1986-98 (2005)] and its OID representation.
obligation:patient:mask:purpose:dissenting-role	urn:oasis:names:tc:xspa:1.0:resource:patient:masked:purpose:dissenting-role	String	Structural Role refer to [ASTM E1986-98 (2005)] and its OID representation.
obligation:patient:mask:results:dissenting-role	urn:oasis:names:tc:xspa:1.0:resource:patient:masked:results:dissenting-role	String	Structural Role refer to [ASTM E1986-98 (2005)] and its OID representation.
obligation:patient:mask:socialhistory:dissenting-role	urn:oasis:names:tc:xspa:1.0:resource:patient:masked:socialhistory:dissenting-role	String	Structural Role refer to [ASTM E1986-98 (2005)] and its OID representation.
obligation:patient:mask:vitals:dissenting-role	urn:oasis:names:tc:xspa:1.0:resource:patient:masked:vitals:dissenting-role	String	Structural Role refer to [ASTM E1986-98 (2005)] and its OID representation.
obligation:patient:mask:advancedirectives:dissenting-subject-id	urn:oasis:names:tc:xspa:1.0:resource:patient:masked:advancedirectives:dissenting-subject-id	String	Provider unique identifier. US Domain this is National Provider Identifier NPI.
obligation:patient:mask>alerts:dissenting-subject-id	urn:oasis:names:tc:xspa:1.0:resource:patient:masked>alerts:dissenting-subject-id	String	Provider unique identifier. US Domain this is National Provider Identifier NPI.
obligation:patient:mask:encounters:dissenting-subject-id	urn:oasis:names:tc:xspa:1.0:resource:patient:masked:encounters:dissenting-subject-id	String	Provider unique identifier. US Domain this is National Provider Identifier NPI.

Attribute ID*	Identifier	Type	Valid Values
obligation:patient:mask:familyhistory:dissenting-subject-id	urn:oasis:names:tc:xspa:1.0:resource:patient:masked:familyhistory:dissenting-subject-id	String	Provider unique identifier. US Domain this is National Provider Identifier NPI.
obligation:patient:mask:functionalstatus:dissenting-subject-id	urn:oasis:names:tc:xspa:1.0:resource:patient:masked:functionalstatus:dissenting-subject-id	String	Provider unique identifier. US Domain this is National Provider Identifier NPI.
obligation:patient:mask:immunizations:dissenting-subject-id	urn:oasis:names:tc:xspa:1.0:resource:patient:masked:immunizations:dissenting-subject-id	String	Provider unique identifier. US Domain this is National Provider Identifier NPI.
obligation:patient:mask:medicalequipment:dissenting-subject-id	urn:oasis:names:tc:xspa:1.0:resource:patient:masked:medicalequipment:dissenting-subject-id	String	Provider unique identifier. US Domain this is National Provider Identifier NPI.
obligation:patient:mask:medications:dissenting-subject-id	urn:oasis:names:tc:xspa:1.0:resource:patient:masked:medications:dissenting-subject-id	String	Provider unique identifier. US Domain this is National Provider Identifier NPI.
obligation:patient:mask:payayers:dissenting-subject-id	urn:oasis:names:tc:xspa:1.0:resource:patient:masked:payayers:dissenting-subject-id	String	Provider unique identifier. US Domain this is National Provider Identifier NPI.
obligation:patient:mask:planofcare:dissenting-subject-id	urn:oasis:names:tc:xspa:1.0:resource:patient:masked:planofcare:dissenting-subject-id	String	Provider unique identifier. US Domain this is National Provider Identifier NPI.
obligation:patient:mask:problems:dissenting-subject-id	urn:oasis:names:tc:xspa:1.0:resource:patient:masked:problems:dissenting-subject-id	String	Provider unique identifier. US Domain this is National Provider Identifier NPI.
obligation:patient:mask:procedures:dissenting-subject-id	urn:oasis:names:tc:xspa:1.0:resource:patient:masked:procedures:dissenting-subject-id	String	Provider unique identifier. US Domain this is National Provider Identifier NPI.
obligation:patient:mask:purpose:dissenting-subject-id	urn:oasis:names:tc:xspa:1.0:resource:patient:masked:purpose:dissenting-subject-id	String	Provider unique identifier. US Domain this is National Provider Identifier NPI.
obligation:patient:mask:results:dissenting-subject-id	urn:oasis:names:tc:xspa:1.0:resource:patient:masked:results:dissenting-subject-id	String	Provider unique identifier. US Domain this is National Provider Identifier NPI.
obligation:patient:mask:socialhistory:dissenting-subject-id	urn:oasis:names:tc:xspa:1.0:resource:patient:masked:socialhistory:dissenting-subject-id	String	Provider unique identifier. US Domain this is National Provider Identifier NPI.
obligation:patient:mask:vitals:dissenting-subject-id	urn:oasis:names:tc:xspa:1.0:resource:patient:masked:vitals:dissenting-subject-id	String	Provider unique identifier. US Domain this is National Provider Identifier NPI.

186 \*Note: Attribute-ID is provided for mapping to pseudo-code in the [XSPA-XACML Example] document.

## 187 2.12 Standard Rules (Normative)

188 At this time no Standard Rule requirements have been defined for this profile.

## 189 2.13 Standard Rules (Non-normative)

190 At this time no optional Rules have been defined for this profile.

## 191 2.14 Obligations (Normative)

192 This profile describes the use of <Obligation> element as optional.

## 193 2.15 Obligations (Non-normative)

194 The <Obligation> element will be used in the XACML response to notify requestor that additional  
195 processing requirements are needed. This profile focuses on the use of obligations to enforce patient  
196 privacy election. The XACML response may contains one or more obligations. Processing of an  
197 obligation is application specific. An <Obligation> may contain the object (resource) action pairing  
198 information. If multiple vocabularies are used for resource definitions the origin of the vocabulary MUST  
199 be identified.

200 The obligation should conform to following structure:

201 urn:oasis:names:tc:xspa:1.0:patient:<action>:<healthcareobject>:<constraint-identifier>

202 The following is an example response obligation segment.

```
203 <xacml:Obligations  
204 xmlns:xacml="urn:oasis:names:tc:xacml:2.0:policy:schema:os" >  
205 <xacml:Obligation  
206 ObligationId="urn:oasis:names:tc:xspa:1.0:patient:masked:vitals:dissenting-  
207 subject-id" FulfillOn="Permit">  
208 </xacml:Obligation>  
209 </xacml:Obligations>
```

## 210 2.16 Examples of Use

211 The following section of this profile provides examples of XACML request and response messages. The  
212 examples are intended to provide additional guidance to implementers of this profile.

213 All XACML request and response attributes are identified by a Uniform Resource Name (URN) from the  
214 vocabulary. This enables seamless mapping of data values between the client interface and policy  
215 services.

216 It is recommended that the SAML 2.0 profile of XACML v2.0 [SAML-XACML20] be used for PEP-PDP  
217 communications. (Note: use [SX20-ASSN-SCH] and [SX20-PROT-SCH] schema files and specification  
218 in 17-Nov-05 Errata version.)

219 Following are the expected SOAP-wrapped request and response messages. Note that request MUST  
220 have a unique ID which is used to map to a unique response as specified in [XACML-CORE]. The  
221 request MAY be returned with the response.

### 222 Sample SOAP SAML XACML Request wrapper:

```
223 <?xml version="1.0" encoding="UTF-8"?>  
224 <soapenv:Envelope  
225 xmlns:soapenv ="http://schemas.xmlsoap.org/soap/envelope/"  
226 xmlns:xsd="http://www.w3.org/2001/XMLSchema"  
227 xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">  
228 <soapenv:Body>  
229 <xacml-samlp:XACMLAuthzDecisionQuery  
230 xmlns:xacml-samlp="urn:oasis:xacml:2.0:saml:protocol:schema:os"  
231 ID="_e064bd912f83c1544fea110307000acf">
```

```

232         IssueInstant="2007-05-21T22:00:36Z"
233         Version="2.0">
234         <xacml-context:Request
235             xmlns:xacml-
236 context="urn:oasis:names:tc:xacml:2.0:context:schema:os">
237             <!-- See [XACML-Request-01] for sample content of this element -->
238             </xacml-context:Request>
239         </xacml-sampl:XACMLAuthzDecisionQuery>
240     </soapenv:Body>
241 </soapenv:Envelope>

```

242 The request message above contains three protocol layers:

- 243 • **soapenv:** is the SOAP layer. A SOAP Envelope contains a SOAP Body.
- 244 • **xacml-sampl:** is the SAML protocol layer, which is enabled by the XACML extension to the SAML  
245 protocol, which is described in **[SAML-XACML-20]** specification and in the **[SX20-PROT-SCH]**  
246 schema. Note that the usual sampl: is not declared here because xacml-sampl: extends sampl: and  
247 will transparently include the sampl: base declarations.
- 248 • **xacml-context:** is the XACML request/response layer which is described in **[XACML-CORE]**.

#### 249 Sample SOAP SAML XACML response wrapper:

```

250 <soapenv:Envelope
251     xmlns:soapenv="http://schemas.xmlsoap.org/soap/envelope/"
252     xmlns:xsd="http://www.w3.org/2001/XMLSchema"
253     xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">
254     <soapenv:Body>
255         <sampl:Response
256             xmlns:sampl="urn:oasis:names:tc:SAML:2.0:protocol"
257             ID="A12345602"
258             Version="2.0"
259             IssueInstant="2007-05-09T00:00:01Z">
260             <sampl:Status>
261                 <sampl:StatusCode
262                     Value="urn:oasis:names:tc:SAML:2.0:status:Success"/>
263             </sampl:Status>
264             <saml:Assertion
265                 xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion"
266                 Version="2.0"
267                 ID="A12345603"
268                 IssueInstant="2007-05-09T00:00:01Z">
269                 <saml:Issuer>xacml.interop.com</saml:Issuer>
270                 <saml:Statement
271                     xmlns:xacml-saml="urn:oasis:xacml:2.0:saml:assertion:schema:os"
272                     xsi:type="xacml-saml:XACMLAuthzDecisionStatementType">
273                     <xacml-context:Response
274                         xmlns:xacml-
275 context="urn:oasis:names:tc:xacml:2.0:context:schema:os">
276                         <!-- See [XACML-Response-01] for sample content of this element --
277 >
278                     </xacml-context:Response>
279                 </saml:Statement>
280             </saml:Assertion>
281         </sampl:Response>
282     </soapenv:Body>
283 </soapenv:Envelope>

```

284 The response message above contains three protocol layers:

- 285 • **soapenv:** is the SOAP layer. A SOAP Envelope contains a SOAP Body.
- 286 • **sampl:** is the SAML Protocol layer, which is explicitly declared this time because in the response  
287 case the xacml extension is lower in the sampl: protocol. In particular, sampl: requires a  
288 saml:Assertion, which in turn includes a saml:Statement. It is within the saml:Statement that the  
289 xacml extension occurs and is referred to as xacml-saml: because it extends the

290 saml:Assertion/saml:Statement with the XACMLAuthzDecisionStatementType. The details are  
291 described in the **[SAML-XACML-20]** specification and the **[SX20-ASSN-SCH]** schema.  
292 • **xacml-context**: is the XACML request/response layer which is described in **[XACML-CORE]**

---

## 293 3 Conformance

### 294 3.1 Introduction

295 The XSPA profile of XACML addresses the following aspects of conformance:

296 This profile describes a minimum vocabulary that must be supported in order to claim conformance.

297 An Implementation of a PDP MUST conform to XACML v2.0 specification.

### 298 3.2 Conformance Tables

299 The following section identifies portions of the profile that MUST be adhered to in order to claim  
300 conformance.

301 Note: “M” is mandatory “O” is optional.

#### 302 3.2.1 Attributes

303 The implementation MUST use the attributes associated with the following identifiers in the way this  
304 profile has defined.

305

Table 3: Conformance Attributes

Identifiers	
urn:oasis:names:tc:xacml:1.0:subject:subject-id	M
urn:oasis:names:tc:xspa:1.0:subject:organization	M
urn:oasis:names:tc:xspa:1.0:subject:organization-id	M
urn:oasis:names:tc:xspa:1.0:subject:hl7:permission	M
urn:oasis:names:tc:xacml:2.0:subject:role	M
urn:oasis:names:tc:xspa:1.0:subject:purposeofuse	M
urn:oasis:names:tc:xacml:1.0:resource:resource-id	M
urn:oasis:names:tc:xspa:1.0:resource:hl7:type	M
urn:oasis:names:tc:xspa:1.0:resource:org:hl7:permissions	M
urn:oasis:names:tc:xspa:1.0:resource:org:role	M
urn:oasis:names:tc:xspa:1.0:resource:patient:hl7:confidentiality-code	M
urn:oasis:names:tc:xspa:1.0:resource:patient:dissenting-subject-id	M
urn:oasis:names:tc:xspa:1.0:resource:patient:dissenting-role	M
urn:oasis:names:tc:xspa:1.0:environment:locality	M
urn:oasis:names:tc:xspa:1.0:subject:npi	O

Identifiers	
urn:oasis:names:tc:xspa:1.0:subject:functional-role	O
urn:oasis:names:tc:xspa:1.0:resource:org:allowed-organizations	O
urn:oasis:names:tc:xspa:1.0:resource:org:hoursofoperation:start	O
urn:oasis:names:tc:xspa:1.0:resource:org:hoursofoperation:end	O
urn:gov:hhs:fha:nhinc:patient-opt-in	O
urn:oasis:names:tc:xspa:1.0:resource:patient:allowed-organizations	O
urn:oasis:names:tc:xspa:1.0:resource:patient:masked:advancedirectives:dissenting-role	O
urn:oasis:names:tc:xspa:1.0:resource:patient:masked:alerts:dissenting-role	O
urn:oasis:names:tc:xspa:1.0:resource:patient:masked:encounters:dissenting-role	O
urn:oasis:names:tc:xspa:1.0:resource:patient:masked:familyhistory:dissenting-role	O
urn:oasis:names:tc:xspa:1.0:resource:patient:masked:functionalstatus:dissenting-role	O
urn:oasis:names:tc:xspa:1.0:resource:patient:masked:immunizations:dissenting-role	O
urn:oasis:names:tc:xspa:1.0:resource:patient:masked:medicalequipment:dissenting-role	O
urn:oasis:names:tc:xspa:1.0:resource:patient:masked:medications:dissenting-role	O
urn:oasis:names:tc:xspa:1.0:resource:patient:masked:payers:dissenting-role	O
urn:oasis:names:tc:xspa:1.0:resource:patient:masked:planofcare:dissenting-role	O
urn:oasis:names:tc:xspa:1.0:resource:patient:masked:problems:dissenting-role	O
urn:oasis:names:tc:xspa:1.0:resource:patient:masked:procedures:dissenting-role	O
urn:oasis:names:tc:xspa:1.0:resource:patient:masked:purpose:dissenting-role	O
urn:oasis:names:tc:xspa:1.0:resource:patient:masked:results:dissenting-role	O
urn:oasis:names:tc:xspa:1.0:resource:patient:masked:socialhistory:dissenting-role	O
urn:oasis:names:tc:xspa:1.0:resource:patient:masked:vitals:dissenting-role	O
urn:oasis:names:tc:xspa:1.0:resource:patient:masked:advancedirectives:dissenting-subject-id	O
urn:oasis:names:tc:xspa:1.0:resource:patient:masked:alerts:dissenting-subject-id	O
urn:oasis:names:tc:xspa:1.0:resource:patient:masked:encounters:dissenting-subject-id	O
urn:oasis:names:tc:xspa:1.0:resource:patient:masked:familyhistory:dissenting-subject-id	O
urn:oasis:names:tc:xspa:1.0:resource:patient:masked:functionalstatus:dissenting-subject-id	O
urn:oasis:names:tc:xspa:1.0:resource:patient:masked:immunizations:dissenting-subject-id	O

Identifiers	
urn:oasis:names:tc:xspa:1.0:resource:patient:masked:medicalequipment:dissenting-subject-id	○
urn:oasis:names:tc:xspa:1.0:resource:patient:masked:medications:dissenting-subject-id	○
urn:oasis:names:tc:xspa:1.0:resource:patient:masked:payers:dissenting-subject-id	○
urn:oasis:names:tc:xspa:1.0:resource:patient:masked:planofcare:dissenting-subject-id	○
urn:oasis:names:tc:xspa:1.0:resource:patient:masked:problems:dissenting-subject-id	○
urn:oasis:names:tc:xspa:1.0:resource:patient:masked:procedures:dissenting-subject-id	○
urn:oasis:names:tc:xspa:1.0:resource:patient:masked:purpose:dissenting-subject-id	○
urn:oasis:names:tc:xspa:1.0:resource:patient:masked:results:dissenting-subject-id	○
urn:oasis:names:tc:xspa:1.0:resource:patient:masked:socialhistory:dissenting-subject-id	○
urn:oasis:names:tc:xspa:1.0:resource:patient:masked:vitals:dissenting-subject-id	○

306

307

308

---

## A. Acknowledgements

309 The following individuals have participated in the creation of this specification and are gratefully  
310 acknowledged:

311 **Participants in the 2009 HIMSS Interoperability Demonstration of the XSPA profile:**

312 Steve Steffensen, Department of Defense  
313 Daniel Dority, Jericho Systems Corporation  
314 Brian McClung, Jericho Systems Corporation  
315 Brendon Unland, Jericho Systems Corporation  
316 Emory Fry, Naval Health Research Center  
317 Anil Saldhana, Red Hat  
318 Dilli Doral, Sun Microsystems  
319 Steven Jarosz, Sun Microsystems  
320 Mike Davis, Veterans Health Administration  
321 Duane DeCouteau, Veterans Health Administration  
322 David Staggs, Veterans Health Administration

323 **XACML TC Members during the development of this specification:**

324 Erik Rissanen, Axiomatics AB  
325 Steve Anderson, BMC Software  
326 Ronald Jacobson, CA  
327 Masum Hasan, Cisco Systems, Inc.  
328 Anil Tappetla, Cisco Systems, Inc.  
329 Tim Moses, Entrust  
330 Michiharu Kudo, IBM  
331 Michael McIntosh, IBM  
332 Ron Williams, IBM  
333 Guy Denton, IBM  
334 Craig Forster, IBM  
335 Richard Franck, IBM  
336 Vernon Murdoch, IBM  
337 Anthony Nadalin, IBM  
338 Bill Parducci, Individual  
339 David Chadwick, Individual  
340 Abbie Barbir, Nortel  
341 Harry Haurly, NuParadigm Government Systems, Inc.  
342 Hal Lockhart, Oracle Corporation  
343 Willem de Pater, Oracle Corporation  
344 Prateek Mishra, Oracle Corporation  
345 Kamalendu Biswas, Oracle Corporation  
346 Rich Levinson, Oracle Corporation  
347 Anil Saldhana, Red Hat  
348 Darran Rolls, SailPoint Technologies  
349 Daniel Engovatov, Stream Dynamics, Inc.  
350 Aravindan Ranganathan, Sun Microsystems  
351 Dilli Arumugam, Sun Microsystems  
352 Seth Proctor, Sun Microsystems  
353 John Tolbert, The Boeing Company  
354 Martin Smith, US Department of Homeland Security  
355 Duane DeCouteau, Veterans Health Administration  
356 David Staggs, Veterans Health Administration

357

## B. Revision History

358

Document ID	Date	Committer	Comment
xspa-xacml-profile-01	09/29/2008	Brett Burley	Initial draft v1.0
xspa-xacml-profile-01	09/29/2008	Craig Winter	QA review / revision v1.1
xspa-xacml-profile-01	10/03/2008	Duane DeCouteau	Obligation, rules, and Snomed CT. v,1,2
xspa-xacml-profile-cd01	10/10/2008	Brett Burley	Formatting as Committee Draft
xspa-xacml-profile-cd-02	10/23/2008	Duane DeCouteau	Action Items, structural roles, HL7 OID, conformance section
xspa-xacml-profile-cd-02	11/05/2008	Craig Winter	QA review / revision v1.3
xspa-xacml-profile-pr-01	11/05/2008	David Staggs	Approved Public Review Draft v1.0
xspa-xacml-profile-pr-02	4/20/2008	David Staggs	Post-Public Review Draft
xspa-xacml-profile-cd-02	6/7/2009	David Staggs	CD prior to Public Review Draft v2.0
xspa-xacml-profile-cd-02	7/2/2009	David Staggs	CD prior to Public Review Draft v3.0
xspa-xacml-profile-cd-03	7/10/2009	David Staggs	Harmonized with XSPA profile of SAML
xspa-xacml-profile-cd-04	7/15/2009	Duane DeCouteau	Final comments TC review

359